mcpprobe

Security overview

How mcpprobe handles your server and your data.

A summary for security reviews. The policies linked at the end are binding; this page adds nothing to them. mcpprobe holds no SOC 2 or ISO 27001 certification.

Reviewed 3 November 2026 · scanner v0.3.5 · mcpprobe.tech/security-overview

What we scan

- MCP servers: authentication and OAuth metadata, tool descriptions and annotations, sessions, transport and error handling.
- 24 passive checks run today. 8 active checks are coming soon and send nothing until they ship.
- We test the server and the protocol, not your prompts or AI model.

Passive only

- Checks never call a tool and never write, change or delete data. They send what a normal client sends, plus a few malformed requests.
- 5 requests a second by default, never more than 10.
- Every request carries the user-agent `mcpprobe/0.3.5 (+https://mcpprobe.tech/scanning-policy)`. Hosted scans come from the addresses at /scanning-ips.json.

Ownership verification

- Hosted scans run only after you publish `mcpprobe-verification=<token>` as a DNS TXT record at `_mcpprobe.<host>`.
- Verification is checked again before every scan and expires after 90 days.
- Unverified servers are never scanned. The one exception is our passive research survey of the public MCP registry and other public MCP server directories, which publishes aggregate figures only.
- Any host can opt out without an account: TXT `mcpprobe-opt-out=all` at `_mcpprobe.<host>`.

Data handling

- The open-source CLI sends us nothing: no telemetry, no tool descriptions, no results.
- Hosted data is processed in London (AWS eu-west-2). We store the request and response for each failed check (tokens and keys redacted), a hash of the tool list, the authorisation record and your account email.
- Evidence is deleted after 30 days (Free), 12 months (Team) or 24 months (Business). Authorisation records are kept for six years.
- TLS 1.2 or later in transit, AES-256 at rest. Sub-processors: AWS, Stripe (billing), Resend (email).
- Tool descriptions go to no third-party AI model unless you turn on the optional judge.
- Free reports are public; Team and Business reports are private to the account.

Accounts

- Sign-in is a single-use email link. The session cookie is httpOnly, Secure and SameSite=Lax.
- Optional two-step sign-in adds a 6-digit code from an authenticator app, with one-time recovery codes.
- Staff who can see account details sign in with a second factor, and each view or export of the account list is logged.
- If a personal-data breach affects hosted customers, we notify them within 72 hours of becoming aware.

Vulnerability disclosure

- Report issues in mcpprobe to security@mcpprobe.tech. We acknowledge within 2 business days, and take no legal action over good-faith research that follows the policy.
- Issues our research finds in other servers are reported privately, with 90 days before any public mention.
- security.txt is published.

Contacts and policies

Security	security@mcpprobe.tech
Scanner traffic	abuse@mcpprobe.tech
Questionnaires	hello@mcpprobe.tech
Policies	mcpprobe.tech/scanning-policy · /security · /privacy · /responsible-disclosure · /trust
Company	mcpprobe is a trading name of ORGANIC VILLAGE(UK) LIMITED, company 11783758, England and Wales.